AMENDMENT TO THE CLAIMS

1.   (Currently Amended) A system for controlling computer access, the system operative to:

control access to use of the computer according to settings specified by an administrator for at least one user of the computer, wherein the administrator can input changes to the settings locally to the computer and remotely from the computer on another computer to which the settings do not apply;

store a list of restricted computer applications;

intercept a message for opening a window associated with a requested computer application, the message intercepted before receipt thereof by an operating system to prevent opening the window;

compare the requested computer application to the list of restricted computer applications;

when the requested computer application is matched to the list of restricted computer applications, then prohibit opening the window associated with the requested computer application [[,]] and automatically terminate ~~thus terminating~~ the requested computer application; and

collect information from the computer on which local computer applications the respective user is attempting to access on the computer, the information being compiled in a report regarding the respective user, the report being made accessible to the administrator from a remote database.

2.   (Original) The system of claim 1, wherein the report includes a duration of time the respective user has accessed a particular computer application.

3.   (Previously Presented) The system of claim 1, wherein the report includes identification of one or more chronological times in which the respective user has accessed a particular computer application.

4.   (Original) The system of claim 1, wherein the report includes the computer applications the respective user is denied access to according to the settings specified by the administrator.

5.   (Original) The system of claim 1, wherein the report includes the computer applications to which the respective user is granted access.

6.   (Original) The system of claim 1, wherein the report is in the form of a web page.

7.   (Original) The system of claim 6, wherein the report provides a mechanism for the administrator to authorize the respective user access to a particular application to which the respective was previously denied access.

8.   (Original) The system of claim 6, wherein the report provides a mechanism for the administrator to prohibit the respective user access to a particular application.

9.   (Canceled)

10.   (Canceled)

11.   (Previously Presented) The system of claim 1, further operative to report unit updates the report with new collected information after an occurrence of at least one particular computer event.

12.   (Original)   The system of claim 11, wherein the particular computer event includes the respective user logging on the computer.

13.   (Original)   The system of claim 11, wherein the particular computer event includes the respective user logging off the computer.

14.   (Original)   The system of claim 11, wherein the particular computer event includes the start up of the computer.

15.   (Previously Presented)   The system of claim 1, further operative to collect additional information on which services of a designated computer application the respective user is attempting to access on the computer, the additional information being compiled in a report regarding the respective user.

16.   (Original)   The system of claim 15, wherein the report further includes a duration of time the respective user has accessed a particular service of the designated computer application.

17.   (Previously Presented) The system of claim 15, wherein the report further includes identification of one or more chronological times in which the respective user has accessed the particular service of the designated computer application.

18.   (Original)   The system of claim 15, wherein the report includes the services the respective user is denied access to according to the settings specified by the administrator.

19.   (Original)   The system of claim 15, wherein the report includes the services the respective user is granted access to according to the settings specified by the administrator.

20.   (Original)   The system of claim 15, wherein the report provides a mechanism for the administrator to authorize the respective user access to a particular service to which the respective user was previously denied access.

21.   (Original)   The system of claim 15, wherein the report provides a mechanism for the administrator to prohibit the respective user access to a particular service to which the respective user was previously granted access.

22.   (Currently Amended) A system for controlling computer access, comprising the system operative to:

specify settings to locally regulate access to use of a computer for at least one user of the computer;

locally control access to use of the computer according to the specified settings, wherein an administrator can input changes to the settings locally to the computer and remotely from the computer on another computer to which the settings do not apply;

store a list of restricted computer applications;

monitor messages from a requested computer application that are directed to an operating system;

intercept a message for opening a window associated with the requested computer application, the message intercepted before receipt thereof by the operating system to prevent opening the window;

compare the requested computer application to the list of restricted computer applications;

when the requested computer application is matched to the list of restricted computer applications, then prohibit opening the window associated with the requested computer application [[,]] and automatically terminate thus terminating the requested computer application;

collect information from the computer on which local computer applications the respective user is attempting to access on the computer, and

compile the information into a report of the respective user, the report being viewable by an administrator of the computer, the report being made accessible to an administrator of the computer from a remote database.

23.   (Previously Presented) The system of claim 22, further operative to specify in the report a duration of time the respective user has accessed a particular computer application.

24.   (Previously Presented) The system of claim 22, further operative to specify, in the report, identification of one or more chronological times in which the respective user has accessed a particular computer application.

25.   (Previously Presented) The system of claim 22, further operative to specify in the report the computer applications the respective user is denied access to according to the settings specified by the administrator.

26.   (Previously Presented) The system of claim 22, further operative to specify in the report the computer applications the respective user is granted access to according to the settings specified by the administrator.

27.   (Original)   The system of claim 22, wherein the report is in the form of a web page.

28.   (Previously Presented) The system of claim 27, further operative to authorize the respective user access to a particular application to which the respective user was previously denied access.

29.   (Previously Presented) The system of claim 27, further operative to prohibit the respective user access to a particular application to which the respective user was previously granted access.

30.   (Canceled)

31.   (Previously Presented) The system of claim 27, further operative to store the report of the respective user.

32.   (Previously Presented) The system of claim 22, further operative to update the report with new collected information after an occurrence of at least one particular computer event.

33.   (Original)   The system of claim 32, wherein the particular computer event includes the respective user logging on the computer.

34.   (Original)   The system of claim 32, wherein the particular computer event includes the respective user logging off the computer.

35.   (Original)   The system of claim 32, wherein the particular computer event includes the start up of the computer.

36.   (Previously Presented) The system of claim 22, further operative to:

        collect additional information on which services of a designated computer application the respective user is attempting to access on the computer; and
        compile the additional information in a report regarding the respective user.

37.   (Original)   The system of claim 36, wherein the report further includes a duration of time the respective user has accessed a particular service of the designated computer application.

38.   (Previously Presented) The system of claim 36, wherein the report further includes identification of one or more chronological times in which the respective user has accessed the particular service of the designated computer application.

39.   (Original)   The system of claim 36, wherein the report includes the services the respective user is denied access to according to the settings specified by the administrator.

40.   (Original)   The system of claim 36, wherein the report includes the services the respective user is granted access to according to the settings specified by the administrator.

41.   (Previously Presented) The system of claim 36, further operative to authorize the respective user to have access to a particular service to which the respective user was previously denied access.

42.   (Previously Presented) The system of claim 36, further operative to prohibit the respective user to have access to a particular service to which the respective user was previously granted access.

43.   (Currently Amended) A method for controlling computer access, comprising:

        specifying settings to locally regulate access to use of a computer for at least one user of the computer;

        locally controlling access to use of the computer according to the specified settings, wherein an administrator can input changes to the settings locally to the computer and remotely from the computer on another computer to which the settings do not apply;

        storing a list of restricted computer applications;

        intercepting a message for opening a window associated with a requested computer application, the message intercepted before receipt thereof by an operating system to prevent opening the window;

        comparing the requested computer application to the list of restricted computer applications;

        when the requested computer application is matched to the list of restricted computer applications, then prohibiting opening the window associated with the requested computer application [[,]] and automatically terminate ~~thus terminating~~ the requested computer application;

collecting information from the computer on which local computer applications the respective user is attempting to access on the computer, and

compiling the information into a report of the respective user, the report being viewable by an administrator of the computer, the report being made accessible to an administrator of the computer from a remote database.

44.   (Previously Presented) The method of claim 43, further comprising:

specifying in the report a duration of time the respective user has accessed a particular computer application.

45.   (Previously Presented) The method of claim 43, further comprising:

specifying, in the report, identification of one or more chronological times in which the respective user has accessed a particular computer application.

46.   (Previously Presented) The method of claim 43, further comprising:

specifying in the report the computer applications the respective user is denied access to according to the settings specified by the administrator.

47.   (Previously Presented) The method of claim 43, further comprising:

specifying in the report the computer applications the respective user is granted access to according to the settings specified by the administrator.

48.   (Original)   The method of claim 43, wherein the report is in the form of a web page.

49.   (Previously Presented) The method of claim 48, further comprising:

authorizing the respective user access to a particular application to which the respective user was previously denied access.

50.   (Previously Presented) The method of claim 48, further comprising:

prohibiting the respective user access to a particular application to which the respective user was previously granted access.

51.   (Canceled)

52.   (Previously Presented) The method of claim 48, further comprising:
        storing the report of the respective user.

53.   (Previously Presented) The method of claim 43, further comprising:
        updating the report with new collected information after an occurrence of at least one particular computer event.

54.   (Original)   The method of claim 53, wherein the particular computer event includes the respective user logging on the computer.

55.   (Original)   The method of claim 53, wherein the particular computer event includes the respective user logging off the computer.

56.   (Original)   The method of claim 53, wherein the particular computer event includes the start up of the computer.

57.   (Previously Presented) The method of claim 43, further comprising:

        collecting additional information on which services of a designated computer application the respective user is attempting to access on the computer, and
        compiling the additional information in a report of the respective user.

58.   (Original)   The method of claim 57, wherein the report further includes a duration of time the respective user has accessed a particular service of the designated computer application.

59.   (Previously Presented) The method of claim 57, wherein the report further includes identification of one or more chronological times in which the respective user has accessed the particular service of the designated computer application.

60.   (Original)   The method of claim 57, wherein the report includes the services the respective user is denied access to according to the settings specified by the administrator.

61.   (Original)   The method of claim 57, wherein the report includes the services the respective user is granted access to according to the settings specified by the administrator.

62.   (Previously Presented) The method of claim 57, further comprising:

        authorizing the respective user to have access to a particular service to which the respective user was previously denied access.

63.   (Previously Presented) The method of claim 57, further comprising:

        prohibiting the respective user to have access to a particular service to which the respective user was previously granted access.